The Definitive Zero Trust Authentication Checklist

BEYOND IDENTITY

Zero trust—the term given to the concept of providing least privileged access to IT resources both on-premise and in the cloud—is the security industry buzzword of the past few years. From hackers purchasing external usernames and passwords to internal actors moving laterally to access off-limits resources, the idea of zero trust is to assume bad actors are exploiting vulnerabilities and to set a course in action to close them.

While many organizations have chosen to upgrade their endpoint detection and response tools and move from virtual private networks (VPNs), which allow lateral movement, to Zero Trust Network Access (ZTNA) or Secure Access Service Edge (SASE) solutions, many are also looking to ensure the users—the identity of the users and the device(s) they are allowed to use—are valid and secure. Marrying identity-centric access to network-centric access is the essence of zero trust.

Zero Trust Authentication, by extension, is designed to thwart identity-centric breaches before they can start, and provides an essential and foundational cornerstone to achieve a zero trust security strategy.

But what goes into a Zero Trust Authentication solution? Through our collaboration with security advocates and leading-edge companies at high risk of attack, we have a comprehensive checklist of the key capabilities needed to achieve Zero Trust Authentication for your extended workforce, contractors, partners, and customers.

What you need for Zero Trust Authentication

- ☐ **Phishing-resistant multi-factor authentication:** First-generation MFA uses phishable factors like one-time passwords, and magic links. These weak factors rely on trusting the user entering in the code is who they say they are. Phishing-resistant MFA uses factors like cryptographic keys and biometrics, which do not rely on trust because the key is tied to the device.

- ☐ **Risk-based policy enforcement:** A robust policy engine lets you ensure that everyone accessing resources meets the security requirements set by the organization, ensuring their identity, tracking their behavior, and ensure the devices used to access resources are allowed—rather than a simple authentication system that trusts that the user identity or their device is enough without consideration of behavior and risk profile. This allows you to block access if there is risky or abnormal behavior detected (like a firewall being turned off) or ask for step-up authentication for high-risk situations (such as logging in from an unmanaged device).

- ☐ **Ability to evaluate device security posture:** Ensuring devices are compliant and meet security standards is critical for Zero Trust Authentication. Traditional MFA doesn't include this critical check and just trusts the device is up to standards of the organization.

- [ ] **Secure passkeys:** Passkeys that form a public-private key pair cryptographically authenticate users via all three authentication factors (possession, knowledge, and inherence) without the need or risk of shared secrets, such as passwords, one-time codes, and SMS text messages—all of which implicitly trust the user and device.
- [ ] **Incorporate risk signals from detection and response security controls:** Zero Trust Authentication leverages the entire security ecosystem by using the tools to be more robust in authentication decisions and truly secure resources. For example, by leveraging tools like CrowdStrike it allows an organization to establish trust in the device and identity and quarantine risky devices. Traditional MFA doesn't utilize all the security tools available to truly verify the secure access of resources.
- [ ] **Integrates with EDR, XDR, and SOC/SIEM:** Zero Trust Authentication needs to share data with other tools in the security ecosystem to improve risk detection so that it can continuously detect abnormal behavior and verify the device regularly. Traditional MFA relies on one-time authentication and trusts that nothing malicious will happen during the user session.
- [ ] **Continuous authentication:** Risk-based access at login alone isn't enough. To achieve Zero Trust Authentication, the solution must continuously verify the user's identity and their authorization to access sensitive resources. This adheres to the zero trust principle of "never trust, always verify."

While the notion of "continuous" may be the furthest down the checklist, we've placed this here since all of the information used to secure initial user authentication must be processed continuously to keep watch for changes that may create vulnerabilities or signal risk of breach and take action, from step up of authentication to verify identity and assess the device to session termination and device quarantine.

Beyond Identity is the leading provider of Zero Trust Authentication, delivering continuous risk-based multi-factor authentication that delivers the level of security assurance required by an organization's security team while simultaneously making the lives of users easier, which is essential for the identity and access management team.

On their own, a passwordless user experience or a phishing-resistant multi-factor solution are not enough to meet the challenge of zero trust, which is why Beyond Identity is driving the industry to Zero Trust Authentication. We provide a phishing-resistant MFA and passwordless user experience that prevents security breaches and offers unparalleled security. Get a demo today.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.